1 PURPOSE

This standard operating procedure (SOP) provides incident response (IR) procedures for the National Aeronautics and Space Administration (NASA) Headquarters (HQ) Computer Incident Response Team (CIRT). The steps outlined in this SOP standardize incident handling at NASA HQ to the NASA Agency standard. This standardization is facilitated by the Office of the Chief Information Officer (OCIO) and the NASA Security Operations Center (NSOC).

2 APPLICABILITY

This SOP is intended for HQ CIRT team members.

3 SCOPE

This SOP provides instruction for responding to IT security events affecting the confidentiality, integrity, and availability of NASA HQ information technology (IT) assets and data. NASA HQ IT assets and data include, but are not limited to, all systems, applications and data provided to HQ employees and contractor staff located in the following locations: 1) NASA HQ, located at 300 E Street SW, Washington, DC 20546; 2) 400 Virginia Avenue SW, Suite 200 and Suite 350, Washington, D.C., 20024; and 3) the InDyne Information Services Facility, located at 200 12th Street South, Suite 200 and Suite 300, Arlington, VA 22202.

In addition, this SOP supports NASA HQ employees and contractor staff remotely connecting to NASA IP space via virtual private network (VPN), Secure Nomadic Access (SNA) and other approved remote connection mechanisms used at NASA HQ.

4 CONSTRAINTS

This SOP includes procedures for organizational action in response to computer security incidents. It does not address physical disruptions to, or the loss of, information, automated information systems, or networks as a result of human error or natural disasters impacting the information infrastructure. These non-cyber events are included in the HQ IT Security Contingency Plan.

5 DEFINITIONS

Computer Incident Response Team (CIRT) – IT Security personnel whose purpose is to promptly and correctly handle an incident so that it can be quickly contained, investigated, and recovered.

Event – An observable, anomalous occurrence not yet assessed that may affect the performance of an information system. Events are aspects of an investigation that can be documented, verified, and analyzed.

Evidence – Data on which to base proof or to establish truth or falsehood.

IMS – Incident Management System. Incident database managed by the NASA Security Operation Center to document, track and analyze qualifying incidents.

Incident – An adverse event or series of events that impact system security or the ability to do business. Incidents indicate an attempted or achieved unauthorized entry or information attack on a NASA system or network.

IT Asset – Information technology asset such as hardware, software, or data.

Personal Identifiable Information (PII) – Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information, which can be used to distinguish or trace an individual's identity, such as his/her name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual.

Vulnerability – A weakness in a system (e.g., system security procedures, hardware, design, or internal controls) that could be exploited.

6 RESPONSIBILITIES

The following table identifies the major roles and responsibilities in the incident response process:

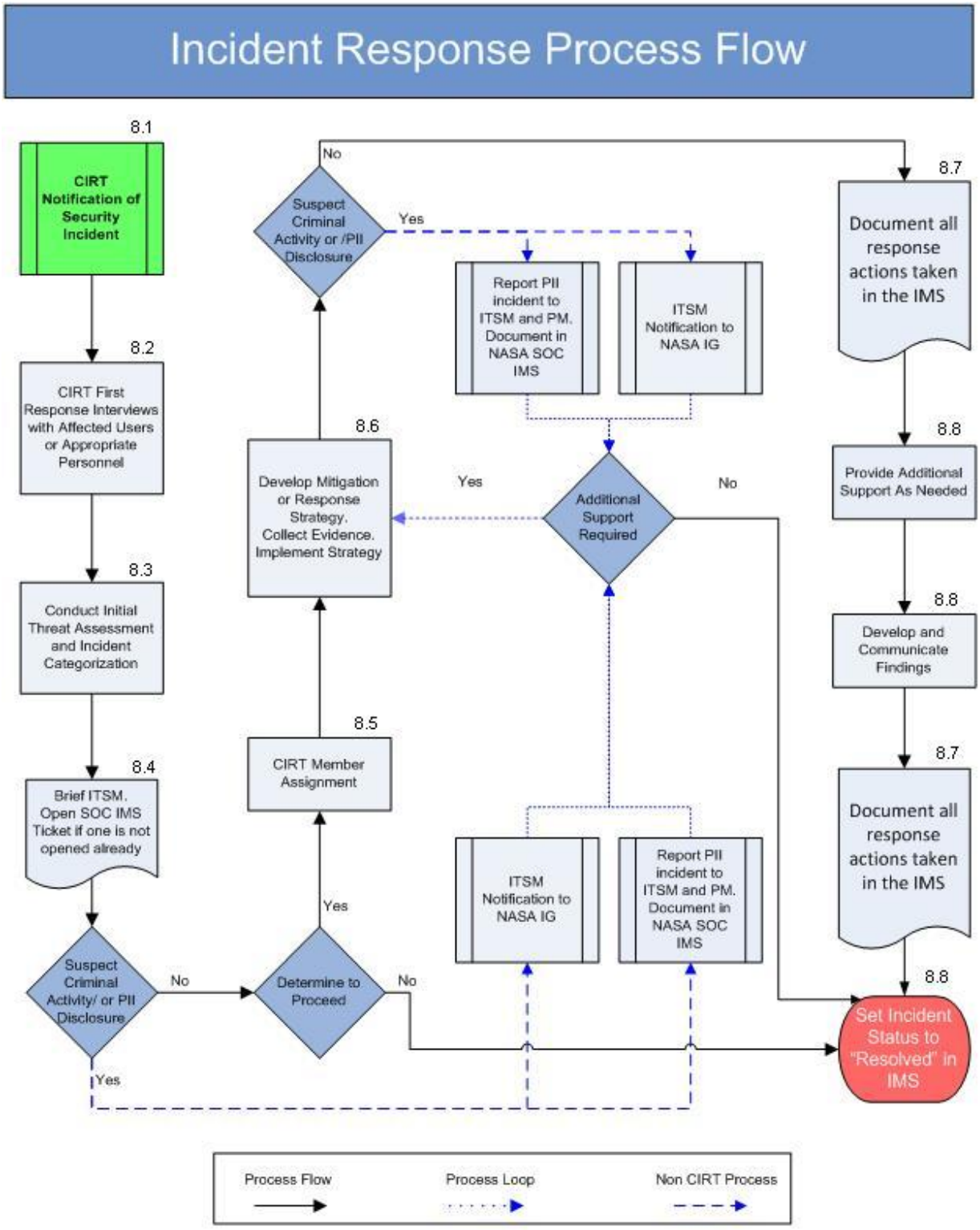
Table 1 – Incident Response Roles & Responsibilities

Role	Responsibilities
CIRT Members	• Verify and identify IT security incidents and events. Document any actions taken in the SOC IMS • Develop and approve triage and incident mitigation strategies and actions • Assess the operational impacts of incidents • Provide recommendations to the Information Technology Security Managers (ITSMs) based on the existing or potential impact on mission caused by the incident/event • Immediately report incidents that potentially involve personally identifiable information (PII) data to the ITSMs and Privacy Manager
NASA Security Operation Center (SOC)	• Delegate Agency and Federal security directives to all NASA Centers including NASA HQ. • Maintain incident status and history in a centralized system called the Incident Management System • Report status of all qualifying incidents to appropriate Agency managers and to third party entities such as the Office of the Inspector General or the Federal Bureau of Investigations as needed. • Report trends and notable incidents to the Office of the Chief Information Officer on a routine and as needed basis.
Headquarters Information Technology Support Services (HITSS) Security Manager	• Assign CIRT member(s) to respond to an incident.
Information Technology Security Manager (ITSM)	• Oversee IR team functional and operational contractual obligations. • Approve incident response actions and mitigation strategies recommended by the CIRT. • Report incidents involving Counter Intelligence (CI) or criminal activity to the Office of Security and Program Protection (OSPP) and NASA Inspector General (IG) respectively.

Role	Responsibilities
HQ Network Operations Center (HNOC)	• Provide the physical location of the NASA HQ system when provided with an Internet Protocol (IP) address • Identify control governing access to the system or network • Capture traffic upon request and review firewall and router logs and provide them to the CIRT and/or the Government upon request • Provide assistance as necessary to shut down physical and logical connection ports • Provide assistance in monitoring or otherwise altering network configurations to meet monitoring needs • Provide status to CIRT and/or the Government on all HNOC IR tasks
Outsourcing Desktop Initiative for NASA (ODIN) Help Desk	• Receive reports of security events/incidents, open Remedy tickets, and initiate the ODIN security response process • Report all discovered events/incidents to the CIRT and/or the responsible Government official • Provide technical assistance with the CIRT initial site visit • Provide a return to service/normal operation for affected ODIN managed systems • Provide status to CIRT and/or Government on all ODIN IR tasks
Privacy Manager	• Perform Privacy Impact Anaysis to determine potential data exposure, theft or otherwise suspicious data breaches • Oversee and advise the CIRT on the specifics of the affected systems and data. Oversee and advise the CIRT on applicable policies, processes, and impacts related to the breach context
HQ Server Operations Center (HSOC)	• Provide the CIRT and/or the appropriate Government official with relevant system logs to investigate incidents • Provide any other CIRT or Government requested historical data associated with relevant affected systems • Assist in the recovery of data from systems that have been affected by security incidents or have otherwise been compromised or are suspected of being compromised by malicious parties
System Administrators	• Coordinate and cooperate with the CIRT on mitigation actions impacting applications, systems, and networks with which the System Administrator interfaces

Role	Responsibilities
Users	• Report ALL suspicious computer events/incidents to the Help Desk or CIRT • Provide input to an Incident/Event Report Log when suspicious activity is detected, or as directed by the CIRT or Systems Administrator • Promptly perform mitigation actions directed by the Help Desk or CIRT • Perform only those mitigation actions directed by the Help Desk or CIRT • Coordinate and cooperate with the Help Desk and CIRT

7 FLOWCHART


Incident Response Process Flow
8.1
CIRT Notification of Security Incident
8.2
CIRT First Response Interviews with Affected Users or Appropriate Personnel
8.3
Conduct Initial Threat Assessment and Incident Categorization
8.4
Brief ITSM. Open SOC IMS Ticket if one is not opened already
Suspect Criminal Activity/ or PII Disclosure
No
Yes
Determine to Proceed
No
Yes
8.5
CIRT Member Assignment
8.6
Develop Mitigation or Response Strategy. Collect Evidence. Implement Strategy
No
Yes
Suspect Criminal Activity or /PII Disclosure
Yes
No
Report PII incident to ITSM and PM. Document in NASA SOC IMS
ITSM Notification to NASA IG
Additional Support Required
ITSM Notification to NASA IG
Report PII incident to ITSM and PM. Document in NASA SOC IMS
8.7
Document all response actions taken in the IMS
8.8
Provide Additional Support As Needed
8.8
Develop and Communicate Findings
8.7
Document all response actions taken in the IMS
8.8
Set Incident Status to "Resolved" in IMS
Process Flow
Process Loop
Non CIRT Process

PROCEDURES

8.1 CIRT Notification of Security Incident

The incident response process begins when a potential IT security finding (event) is discovered and reported. A security event may be identified and reported for investigation via multiple avenues:

- ODIN Help Desk
- System user or coworker
- Automated tools (HQ Intrusion Detection System (IDS) or antivirus (AV) software)
- NASA SOC notification
- NASA Integrated Services Network (NISN) IT Security report
- ITSM

Once a security event is identified, it is reported to the ODIN Help Desk and a ticket is created.

When an incident is reported to the ODIN Help Desk, they will notify the CIRT (if the CIRT is not the original reporting source) according to procedures established in ODIN-HDP-NHQ-075, NHQ IT Security Reporting.

8.2 CIRT Notification: First Responders

The CIRT provides 24 hour support for the identification and mitigation of all IT security incidents within NASA HQ's IT infrastructure and IP space. The HQ ITSM will update and maintain a call down roster with current telephone numbers of individuals responsible for responding to security incidents. This roster is provided to the ODIN Help Desk as well as the NASA SOC.

8.2.1 Prime Time Support:

During the hours of 6:00 AM until 6:00 PM Monday through Friday, except for holidays, the CIRT will be available to support onsite identification and mitigation of incidents.

8.2.2 Weekend and Holiday Support:

To contact a CIRT member after hours, use the procedures as stated in ODIN-HDP-NHQ-075, NASA Headquarters (NHQ) IT Security Reporting. During non-Prime Time hours the First Responder shall respond to a page, the Help Desk, or Government notification within 15 minutes. Upon receiving the incident report, a CIRT member will contact persons associated with the incident to gather information. Persons contacted may include ODIN personnel, the affected user, and his/her supervisor. If required, a CIRT member will arrive on site within two hours for after hour occurrences (weekdays from 6 PM to 6 AM, and weekends and holidays) or as advised by the ITSM.

8.2.3 First Responder Actions

During the initial response, the First Responder will obtain the following information:

- Date of the event.
- Time of the event including the time zone.
- Who or what reported the event. If a person reported the event, include his/her full name, location, telephone number, and email. If an automated system reported the event, include the name of the software package.
- A determination, if possible, of whether or not PII is involved.
- Identification of the host(s) that the event is related to/occurred on. If possible, include the hardware manufacturer, operating system type and version, name of the host, property number, physical location of the host, host or CPU ID of the host, network address of the host, and media access control (MAC) address. If the host has a modem connected to it, document the telephone number of the connected line or the wall jack number.
- Provide a detailed description of the event.

The First Responder will use the NASA SOC Incident Management System to document information obtained during the initial response action as well as later from interviews and analysis of any data collected during the investigation.

8.3 Initial Threat Assessment

NASA HQ CIRT will respond to incidents that meet incident categorizations as defined by the United States Computer Emergency Readiness Team (USCERT) and NASA Procedural Requirements (NPR) 1600.1. The initial threat assessment and incident categorization is based on the Federal Agency Incident Categories as defined by National Institute of Standards and Technology Special Publication (NIST SP) 800-61, Computer Security Incident Handling Guide and is supplemented, as necessary, by the NASA OCIO through policy directives enacted by the NASA SOC.

Table 2 below will be used for incident categorization. It is important to note that some incidents may involve multiple categories. Such incidents should be categorized based on the transmission mechanism.

TABLE 2

Federal Agency Incident Categories

Category	Name	Description
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses. The nature of CAT 0 incidents will vary depending on the corresponding type of exercise or directive from Federal officials.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource. Unauthorized access is typically gained through the exploitation of operating system or application vulnerabilities, the acquisition of usernames and passwords, or social engineering. The following are examples of CAT 1 – "Unauthorized Access" incidents: • Root compromise • User compromise • Website defacements
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources such as central processing units (CPUs), memory, bandwidth, and disk space. This activity includes being the victim or participating in the DoS. An attacker may employ one or more of the following methods to deploy a DoS attack: • Using all available network bandwidth by generating unusually large volumes of traffic. • Sending malformed TCP/IP packets to a server so that its operating system will crash. • Sending illegal requests to an application to crash it. • Making many processor-intensive requests so that the server's processing resources are fully consumed (e.g., requests that require the server to encrypt each reply). • Establishing many simultaneous login sessions to a server so that other users cannot start login sessions. • Broadcasting on the same frequencies used by a wireless network to make the network unusable. • Consuming all available disk space by creating many large files.

Category	Name	Description
CAT 3	Malicious Code	Malicious code (e.g., virus, worm, Trojan horse, or other code-based malicious entity) incidents may include a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or the confidentiality, integrity, and availability of the victim's data, applications, or operating system. Generally, malicious code is designed to perform these nefarious functions without the system user's knowledge. The following are examples of CAT 3 – "Malicious Code" incidents: • Successful virus/worm infection • Introduction of a virus/worm into a network • Detection and elimination of malicious logic before infestation • Installation of key loggers • Malware or spyware installation Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus software.
CAT 4	Misuse	A person violates acceptable computing use policies. The following are examples of CAT 4 – "Improper Usage" incidents: • Misuse of resources • Spam email • Fraudulent email • Social Engineering
CAT 5	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. The following are examples of CAT 5 – "Scans/Probes/Attempted Access" incidents: • Scanning of unclassified, non-critical systems • Scanning of classified or critical systems
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. CAT 6 incidents will be initially treated as a CAT 1 incident until further assessment or investigation accurately determines the appropriate category to be assigned.
CAT 7	Non-Incident	*After investigation it was determined no incident occurred.*

8.4 Incident Response Briefing

The First Responder will contact the ITSM using the numbers listed in the Incident Response Call List. The IR Call List is maintained by HITSS Security and distributed separately to all applicable personnel as Sensitive But Unclassified (SBU) data. If an ITSM cannot initially be reached, the First Responder will contact a civil service manager using the call-down structure as identified in the IR Call List. The First Responder will brief the contacted ITSM/civil service manager on the incident, provide an initial assessment of the scope and recommended response strategy, and open an incident ticket in the IMS as necessary. This includes immediately informing the ITSM of any findings that may imply criminal activity or the misuse of PII data.

If criminal activity is indicated or suspected, the ITSM will contact the appropriate agency as prescribed by his/her procedures for analysis. Additional support and investigation or mitigation will be conducted at the discretion of the ITSM.

If PII information appears to be involved, the ITSM will likely direct the First Responder to contact the HQ Privacy Manager using the numbers listed in the IR Call List. If one of the ITSMs cannot initially be reached, the First Responder should immediately attempt to contact the HQ Privacy Manager.

8.5 Team Member Assignment

After briefing the ITSM, the First Responder will contact and brief the HITSS Security Manager. The HITSS Security Manager will notify and officially assign the appropriate CIRT security engineer to lead the case. The First Responder is responsible for providing a briefing on what is known about the incident to this point.

Once assigned, the CIRT lead will be the primary point of contact for documenting and providing all information regarding the case. The CIRT lead will have as broad a view as possible of the environment in which the incident occurred and be trained in incident response procedures. Throughout the incident response process, the CIRT lead will maintain communication with other CIRT members and ITSMs as necessary to report time-sensitive information as determined by the severity of the incident and program manager guidance. Information dissemination regarding an investigation is limited to “need to know” personnel only.

8.6 Incident Processing, Evidence Collection, and Containment

The CIRT will identify that an incident has occurred or is occurring, verifying that the situation is not the result of a misinterpretation or error in judgment. The CIRT lead will brief the ITSMs on any proposed response and mitigation actions and perform the appropriate measures approved by the ITSM. Mitigation and response will vary depending on incident categorization, mission impact, and criticality of the affected systems or resources.

If the incident is not the result of an authorized use violation (CAT4), care will be given to keep the user informed of the status of their system. If the system needs to be removed from service for further analysis two remedy tickets will be opened by the First Responder. One will be opened to track the ensuing investigation and document

corrective action for the user's computer; and the other ticket will request an expedited loaner for the affected user. The user will be given a leave behind document (see Appendix A) containing both ticket numbers and instructions to call the helpdesk for status updates. A member of the CIRT team will leave contact info in case any additional questions or concerns arise.

If evidence of criminal activity is detected at any time during the investigation, an ITSM must be contacted immediately before proceeding. The ITSM will contact the appropriate agency as prescribed by specific HQ procedures to address forensic analysis and disposition. Additional support and investigation or mitigation will only be conducted at the direction of the ITSM in consultation with the criminal investigator. Evidence collected during the course of the investigation should always be handled as though it may be used for prosecution of an individual or entity in a criminal case with the preservation of "best evidence" in mind.

8.6.1 CAT 0 – Exercise/Network Defense Testing

CAT 0 incidents require the CIRT security engineer(s) assigned to follow assessment and mitigation procedures per ITSM direction.

8.6.2 CAT 1 – Unauthorized Access

The CIRT security engineer(s) responding to a CAT 1 incident may conduct the following actions:

1. Interview the user and appropriate personnel, including the user's supervisor, system administrators, or anyone involved in the initial discovery of the incident.
2. Record system ID information including system tag #, make and model, location, and user name.
3. Coordinate with the NOC to ensure that local and perimeter firewall policies have not been modified and that additional ports have not been opened.
4. Check the IDS log for suspicious outbound/inbound communication.
5. Run Mandiant scripts to obtain the following information:

Redacted

6. Collect pertinent antivirus information including the current virus definition file date, program version, items in quarantine, scan history, and risk history.
7. Take note of open applications, running processes, websites the user may have visited before and during the incident, and programs in use.
8. Locate and capture temporary user data (e.g., system and security logs, Internet and system history files, cache, and Internet and system temp directories). Collect all the data and take desktop screenshots as necessary.
9. Maintain a detailed work log and notes of dates, times, and who did what before, during, and after the alleged incident or when anomalous conditions were noticed.

10. Update the Agency IMS system with pertinent information.
11. Additional actions may include the following:
    - Isolating the affected system(s). Complete the Equipment & Data tracking portion of the IR Form if the computer or data is removed from service.
    - Identifying the system security plan(s) for the affected device(s) to determine the system's security plan boundary.
    - Per the direction of the ITSM, removing the original hard drive from the system to secure it as evidence.
    - Creating a dd image of the compromised host's hard drive for additional forensic analysis. Refer to the latest disk imager operator's manual for assistance.

8.6.3 CAT 2 – Denial of Service (DoS)

The CIRT security engineer(s) responding to a CAT 2 incident may conduct the following actions:

1. Interview the user and appropriate personnel, including the user's supervisor, system administrators, or anyone involved in the initial discovery of the alleged incident.
2. Record system ID information including system tag #, make and model, location, and user name.
3. Coordinate with the NOC to ensure that local and perimeter firewall policies have not been modified and access control lists (ACLs) have not been modified.
4. Check the IDS log for suspicious outbound/inbound communication.
5. Take note of open applications, websites the user may have visited before and during the incident, and programs in use.
6. Contact the NOC and provide all information necessary (e.g., ip address, host name, etc.) to monitor/capture network traffic to identify entry points and affected nodes.
7. Maintain a detailed work log and notes of dates, times, and who did what before, during, and after the alleged incident or when anomalous conditions were noticed.
8. Update the Agency IMS with pertinent information.
9. Additional actions may include the following:
    - Isolating the affected system(s). Complete the Equipment & Data tracking portion of the IR Form if the computer or data is removed from service
    - Determining the system's security plan boundary.
    - Running Mandiant scripts.

8.6.4 CAT 3 – Malicious Code

The CIRT security engineer(s) responding to a CAT 3 incident may conduct the following actions:

1. Interview the user and appropriate personnel, including the user's supervisor, system administrators, or anyone involved in the initial discovery of the incident.
2. Record system ID information including system tag #, make and model, location, and user name.
3. Coordinate with the NOC to ensure that local and perimeter firewall policies have not been modified and that additional ports have not been opened.
4. Check the IDS log for suspicious outbound/inbound communication.
5. Run Mandiant scripts to obtain the following information:

Redacted

6. Collect pertinent antivirus information including the current virus definition file date, program version, items in quarantine, scan history, and risk history.
7. Take note of open applications, running processes, websites the user may have visited before and during the incident, and programs in use.
8. Locate and capture temporary user data (e.g., system and security logs, Internet and system history files, cache, and Internet and system temp directories). Collect all the data and take desktop screenshots as necessary.
9. Maintain a detailed work log and notes of dates, times, and who did what before, during, and after the alleged incident or when anomalous conditions were noticed.
10. Update the Agency IMS with pertinent information.
11. Additional actions may include the following:
    - Isolating the affected system(s). Complete the Equipment & Data tracking portion of the IR Form if the computer or data is removed from service.
    - Identifying the system security plan(s) for the affected device(s) to determine the system's security plan boundary.
    - Per the direction of the ITSM, removing the original hard drive from the system to secure it as evidence.
    - Creating a dd image of the compromised host's hard drive for additional forensic analysis. Refer to the latest disk imager operator's manual for assistance.

8.6.5 CAT 4 – Improper Usage

The CIRT security engineer(s) responding to a CAT 4 incident may conduct the following actions:

1. Interview the user and appropriate personnel, including the user's supervisor, system administrators, or anyone involved in the initial discovery of the alleged incident.
2. Record system ID information including system tag #, make and model, location, and user name.
3. Coordinate with the NOC to ensure that local and perimeter firewall policies have not been modified and that additional ports have not been opened.
4. Check the IDS log for suspicious outbound/inbound communication.
5. Run Mandiant scripts to obtain the following information:
    6. **Redacted**
7. Collect pertinent antivirus information including the current virus definition file date, program version, items in quarantine, scan history, and risk history.
8. Take note of open applications, websites the user may have visited before and during the incident, and programs in use.
9. Locate and capture temporary user data (e.g., system and security logs, Internet and system history files, cache, and Internet and system temp directories). Collect all the data and take desktop screenshots as necessary.
10. Maintain a detailed work log and notes of dates, times, and who did what before, during, and after the alleged incident or when anomalous conditions were noticed.
11. Update the Agency IMS with pertinent information.
12. The following are response actions for specific CAT 4 – "Improper Usage" incidents:
    - Misuse of resources:
        - If potential criminal activity is suspected, immediately notify an ITSM.
        - Provide forensic analysis support as necessary.
    - Spam/fraudulent email:
        - Report the offending email address to **abuse@hq.nasa.gov**.
        - Block the offending site/host/ip address using SurfControl/Websense. Refer to current SurfControl guidelines for further instruction.
    - Social Engineering (phishing):
        - Report the offending email address to **abuse@hq.nasa.gov**.
        - Block the offending site/host/ip address using SurfControl/Websense. Refer to current SurfControl guidelines for further instruction.
        - Immediately notify the ITSMs if the incident involves someone impersonating a NASA employee or contractor.

13. Additional actions may include the following:
    - Isolating the affected system(s). Complete the Equipment & Data tracking portion of the IR Form if the computer or data is removed from service.
    - Identifying the system security plan(s) for the affected device(s) to determine the system's security plan boundary.

8.6.6 CAT 5 – Scans/Probes/Attempted Access

The CIRT security engineer(s) responding to a CAT 5 incident may conduct the following actions:

1. Interview the user and appropriate personnel, including the user's supervisor, system administrators, or anyone involved in the initial discovery of the alleged incident.
2. Record system ID information including system tag #, make and model, location, and user name.
3. Coordinate with the NOC to ensure that local and perimeter firewall policies have not been modified and that additional ports have not been opened.
4. Check the IDS log for suspicious outbound/inbound communication.
5. Run Mandiant scripts to obtain the following information:

   Redacted
6. Take note of open applications, websites the user may have visited before and during the incident, and programs in use.
7. Locate and capture temporary user data (e.g., system and security logs, Internet and system history files, cache, and Internet and system temp directories). Collect all the data and take desktop screenshots as necessary.
8. Maintain a detailed work log and notes of dates, times, and who did what before, during, and after the alleged incident or when anomalous conditions were noticed.
9. Update the Agency IMS with pertinent information.
10. The following are response actions for specific CAT 5 - "Scans/Probes/Attempted Access" incidents:
    - Contact the NOC and provide all information necessary (e.g., ip address, host name, etc.) to conduct firewall and ACL log analysis.
    - If incoming traffic is allowed, contact the NOC and provide all information necessary (e.g., ip address, host name, etc.) to begin monitoring and capturing the traffic.
    - Contact the NOC and provide all information necessary (e.g., ip address, host name, etc.) to determine the physical location of the connected/communicating node.

11. Additional actions may include the following:
    - Isolating the affected system(s). Complete the Equipment & Data tracking portion of the IR Form if the computer or data is removed from service.
    - Identifying the system security plan(s) for the affected device(s) to determine the system's security plan boundary.
    - Blocking the offending site/host/ip address using SurfControl/Websense. Refer to current SurfControl guidelines for further instruction.

8.6.7 CAT 6 – Investigation

Category 6 incidents refer to unconfirmed incidents that are potentially malicious or anomalous activity and that warrant further review. A CAT 6 incident investigation will determine the appropriate category to be assigned. The CIRT security engineer(s) responding to a CAT 6 incident may conduct the following actions:

1. Interview the user and appropriate personnel, including the user's supervisor, system administrators, or anyone involved in the initial discovery of the alleged incident.
2. Record system ID information including system tag #, make and model, location, and user name.
3. Coordinate with the NOC to ensure that local and perimeter firewall policies have not been modified and that additional ports have not been opened.
4. Check the IDS log for suspicious outbound/inbound communication. Run Mandiant scripts to obtain the following information:

   Redacted
5. Collect pertinent antivirus information including the current virus definition file date, program version, items in quarantine, scan history, and risk history.
6. Take note of open applications, websites the user may have visited before and during the incident, and programs in use.
7. Locate and capture temporary user data (e.g., system and security logs, Internet and system history files, cache, and Internet and system temp directories). Collect all the data and take desktop screenshots as necessary.
8. Maintain a detailed work log and notes of dates, times, and who did what before, during, and after the alleged incident or when anomalous conditions were noticed.
9. Update the Agency IMS with pertinent information.
10. Complete the Equipment & Data tracking portion of the IR Form if the computer or data is removed from service.
11. Additional actions, depending on the appropriate category assigned to the incident, may include the following:

- Isolating the affected system(s). Complete the Equipment & Data tracking portion of the IR Form if the computer or data is removed from service.
- Determining the system's security plan boundary.
- Running Mandiant scripts.
- Identifying the system security plan(s) for the affected device(s) to determine the system's security plan boundary.
- Blocking the offending site/host/ip address using SurfControl/Websense. Refer to current SurfControl guidelines for further instruction.
- Removing the original hard drive from the system to secure it as evidence.
- Creating a dd image of the compromised host's hard drive for additional forensic analysis. Refer to the latest disk imager operator's manual for assistance.

8.7 Incident Management System

All information collected throughout the incident response life cycle is entered into the NASA SOC IMS. It is integral to the investigation that all evidence is identified and properly secured to maintain its integrity. The ITSMs may review the information provided by the CIRT for quality assurance.

8.8 Additional Reporting, Communication, and Closure

The CIRT will finalize all of the information gathered, incident assessments, and proposed response strategies in the NASA SOC IMS ticket and change incident status to "resolved". Completion times will vary depending on the size and scope of the incident. The NASA SOC or the ITSMs may respond with approval or with any comments, questions, or requirements for additional support. If necessary, additional incident response support will be provided by the CIRT as requested by SOC staff or ITSMs.

9 INCIDENT RESPONSE TRAINING AND TESTING

HITSS Security will train its personnel in their incident response roles and responsibilities with respect to information systems and provide refresher training, at a minimum, on an annual basis. Incident response training dates, team member attendance, and topics presented will be documented (see Appendix C – Incident Response Training Roster).

HITSS Security will test the CIRT's response capability for NASA HQ at least annually using simulated IR events taken from lessons learned of past incidents in order to measure training retention, performance, quality, and overall effectiveness of the CIRT. Test results will be recorded on the Record of Incident Response Plan Testing (Appendix D).

10 RECORDS RETENTION

Record Title	Retention Organization	Retention Period	Disposition
Incident Management System	NASA SOC	Per NPR 1441.1D requirements	Per NPR 1441.1D requirements

11 RELATED DOCUMENTS

ITS-SOP-015	Procedures for Agency IT Security Incident Classification and Reporting
NIST SP 800-61	Computer Security Incident Handling Guide
NPR 2810.1A	Procedural Requirements Security of Information Technology
NPR 1600.1	NASA Security Program Procedural Requirements
NFS 1852.204-76	Security Requirements for Unclassified Information Technology Resources
ODIN-HDP-NHQ-075	NHQ IT Security Reporting

12 REVISION HISTORY

REVISION HISTORY		
Revision	**Description of Change**	**Effective Date**
1.0	Original	8/6/2007
2.0	Major rewrites, included appendices	3/3/2008
3.0	Major rewrites	1/25/2011

13 GLOSSARY OF ACRONYMS

Acronym	Description
AV	Antivirus
BRT	Breach Response Team
CIRT	Computer Incident Response Team
CPU	Central Processing Unit
DoS	Denial of Service
FIPS	Federal Information Processing Standard
HITSS	Headquarters Information Technology Support Services
HQ	Headquarters
HNOC	HQ Network Operations Center
HSOC	HQ Server Operations Center
IDS	Intrusion Detection System
IG	Inspector General
IMS	Incident Management System
IP	Internet Protocol
IR	Incident Response
IT	Information Technology
ITSM	Information Technology Security Manager
MAC	Media Access Control
NASA	National Aeronautics and Space Administration
NASA SOC	NASA SECURITY OPERATIONS CENTER
NFS	NASA FAR Supplement
NHQ	NASA Headquarters
NISN	NASA Integrated Services Network
NIST	National Institute of Standards and Technology
NPR	NASA Procedural Requirements
ODIN	Outsourcing Desktop Initiative for NASA
OSPP	Office of Security and Program Protection
PII	Personal Identifiable Information
SBU	Sensitive But Unclassified
SNA	Secure Nomadic Access
SOP	Standard Operating Procedure
SP	Special Publication
USCERT	United States Computer Emergency Readiness Team
VPN	Virtual Private Network

Appendix A

Urgent IT Notice

Dear _____:

Sorry we missed you during our recent customer outreach. Our records indicate that your computer may have been the victim of a malware or virus incident. We have taken your computer back to our security office and are currently examining it.

If you require a laptop loaner and a ticket for a loaner has not yet been created for you, please contact the ODIN help desk (202-358-4357) to create a ticket. Please be assured that we at HITSS Security are working to resolve this issue in a timely manner.
You may contact the Help Desk to get the status of your computer or the loaner. Please reference the following ticket numbers:

Your Computer – Ticket# _____

Loaner Computer – Ticket# _____

I have included my contact information and a business card for your convenience. Please feel free to contact me with any questions or concerns you may have.

Sincerely,

H.I.T.S.S. Security
Office- 202-552-
Email-

Appendix B - Equipment and DATA Tracking (Example)

Incident: _____

Item: _____

Transferred From							Transferred To				
Date	Time	Name (print)	Name (sign)	Location	Organization	Contact	Name (print)	Name (sign)	Location	Organization	Contact

Appendix C – Incident Response Training Roster (Example)

Class Name:	Trainer:
Date/Time of Class:	Location:

NASA HQ Incident Response Training Roster

Date	Name	Organizational Role	Signature

Appendix D – Record of Incident Response Plan Testing (Example)

Record of Incident Response Plan Testing

National Aeronautics & Space Administration

NASA Headquarters

Plan testing is a critical element of a viable incident response capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the CIRT team to provide timely and effective incident response.

To comply with NIST SP 800-53 and HITSS contract metrics, the incident response plan shall be tested at least annually. The plan shall also be tested more frequently when there has been any significant change to the incident response process.

Plan Test date_____

Test Type(s)_____
(Test types include: checklist, tabletop review, document review simulation)

Test Type Justification:
(Provide a brief explanation of why this test type was chosen)

Incident Response plan testing team:

Attendees	Organizational Title	Team Role	Extension

Appendix E

Incident Response Plan Test Findings

1. **Finding:**

   Action required:

   Responsible team member:

2. **Finding:**

   Action required:

   Responsible team member:

3. **Finding:**

   Action required:

   Responsible team member:

4. **Finding:**

   Action required:

   Responsible team member:

5. **Finding:**

   Action required:

   Responsible team member:

6. **Finding:**

   Action required:

   Responsible team member: